On kaleidoscopic pseudo-randomness of finite Euclidean graphs

Le Anh Vinh

Mathematics Department

Harvard University

Cambridge, MA 02138, US

August 3, 2008

Abstract

D. Hart, A. Iosevich, D. Koh, S. Senger and I. Uriarte-Tuero (2008) showed that the distance graphs has kaleidoscopic pseudo-random property, i.e. sufficiently large subsets of d-dimensional vector spaces over finite fields contain every possible finite configurations. In this paper we study the kaleidoscopic pseudo-randomness of finite Euclidean graphs using probabilistic methods.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements where $q \gg 1$ is an odd prime power. For a fixed $a \in \mathbb{F}_q^*$, the distance graph $G_q(a)$ (also known as finite Euclidean graphs in [7]) in $\mathbb{F}_q^d$ is defined as the graph with vertex set $\mathbb{F}_q^d$ and the edge set

$$E = \{(x, y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d \mid x \neq y, ||x - y|| = a\},$$

where $||.||$ is the analogue of Euclidean distance $||x|| = x_1^2 + \ldots + x_d^2$.

In other words, consider the set of colors $L = \{c_1, \ldots, c_{q-1}\}$ corresponding to elements of $\mathbb{F}_q^*$. We color the complete graph K_{q^d} with vertex set $\mathbb{F}_q^d$ by $q - 1$ colors such that $(x, y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d$ is colored by the color c_i if $||x - y|| = i$. Denote this resulting family of graphs, with respect to the above coloring, by G_q^Δ where q runs over powers of odd primes.

In [7], Medrano et al. studied the spectrum of these graphs and showed that these graphs are asymptotically Ramanujan graphs. In [2], Bannai, Shimabukuro and Tanaka showed that the distance graphs over finite fields are always asymptotically Ramanujan

for a more general setting (i.e. they replace the Euclidean distance above by nondegenerated quadratic forms). The author recently applied these results to several interesting combinatorial problems, for example to tough Ramsey graphs (with P. Dung) [8], to the Erdös distance problem [9], to integral graphs (with Si Li) [6], also to a Szemeredi-Trotter type theorem and to a sum-product estimate [10] (see [11] for related results).

The definition of kaleidoscopic pseudo-randomness below follows Hart et al. [3]. We say that the family of graphs $\{G_j\}_{j=1}^{\infty}$ with the sets of colors $L_j = \{c_j^1, c_j^2, \ldots, c_j^{|L_j|}\}$ and the edge set $\mathcal{E}_j = \bigcup_{i=1}^{|L_j|} \mathcal{E}_j^i$, with $\mathcal{E}_j^i$ corresponding to the color c_j^i, is kaleidoscopically pseudo-random if there exist constants $C, C' > 0$ such that the following conditions are satisfied:

•
$$|G_j| \to \infty \text{ as } j \to \infty. \tag{1.1}$$

• For any j and $1 \leqslant i, i' \leqslant |L_j|$ then

$$\frac{1}{C'}|\mathcal{E}_j^{i'}| \leqslant |\mathcal{E}_j^i| \leqslant C'|\mathcal{E}_j^{i'}|. \tag{1.2}$$

• G_j is asymptotically complete in the sense that

$$\lim_{j \to \infty} \frac{\binom{|G_j|}{2} - \sum_{i=1}^{|L_j|} |\mathcal{E}_j^i|}{\binom{|G_j|}{2}} = 0. \tag{1.3}$$

• If $1 \leqslant k - 1 \leqslant n$ and $L_j' \subset L_j$, with $|L_j'| \leqslant |L_j| - \binom{k}{2} + n$, then any subgraph H of G_j of order

$$\geqslant C|G_j|^{\frac{k-1}{k}}|L|^{\frac{n}{k}}, \tag{1.4}$$

contains every possible subgraph with k vertices and n edges with an arbitrary edge color distribution from L_j'.

In [3], Hart et al. systematically studied various properties of the distance graph. Using Fourier analysis, they proved the following result (see [3] for the motivation and applications of this result).

Theorem 1.1 *([3]) The family of graph $\{G_q^{\Delta}(d)\}$ is kaleidoscopically pseudo-random.*

The first three items in the definition of kaleidoscopically pseudo-randomness above are easy special cases of the following lemma (which is implicit in several papers, for example, see [3, 4, 7, 9]).

Lemma 1.2 *(Lemma 1.2 in [3]) For any $t \in \mathbb{F}_q$, then*

$$|\{(x,y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d : ||x - y|| = t\}| = \begin{cases} (2 + o(1))q^{2d-1} & \text{if } d = 2, t = 0 \\ (1 + o(1))q^{2d-1} & \text{otherwise.} \end{cases} \tag{1.5}$$

where $o(1)$ means that the quantity goes to 0 as q goes to infinity.

Hart et al. ([3]) derived the item (1.4) from the following estimate (This estimate is just a graph theoretic translation of Theorem 1.4 in [3]).

Theorem 1.3 *Consider the color set $L = \{c_1, \ldots, c_{q-1}\}$ coressponding to elements of $\mathbb{F}_q^*$. Color the complete graph K_{q^d} by the Euclidean distance as the above. Let $E \subset \mathbb{F}_q^d$, $d \geq 2$. Suppose that $1 \leq k - 1 \leq n \leq d$ and*

$$|E| \geq Cq^{d\frac{k-1}{k}} q^{\frac{n}{k}} \tag{1.6}$$

with a sufficiently large constant $C > 0$. Then for any subgraph H with k vertices and n edges with an arbitrary edge color distribution from $L' \subset L$ ($|L'| \leq |L| - \binom{k}{2} + n$), we have

$$(1 + o(1))|E|^k q^{-n} \tag{1.7}$$

copies of H (with vertex ordering) in E.

In this paper, we will study more general families of distance graphs. Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. The finite Euclidean graph $E_q(n, Q, a)$ is defined as the graph with vertex set $\mathbb{F}_q^d$ and the edge set

$$E = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid x \neq y, Q(x - y) = a\}. \tag{1.8}$$

Similarly, consider the set of colors $L = \{c_1, \ldots, c_{q-1}\}$ corresponding to elements of $\mathbb{F}_q^*$. We color the complete graph K_{q^d} with vertex set $\mathbb{F}_q^d$ by $q - 1$ colors such that $(x, y) \in \mathbb{F}_q^d \times \mathbb{F}_q^d$ is colored by the color c_i if $Q(x - y) = i$. Denote this resulting family of graphs, with respect to this coloring, by G_q^Q where q runs over powers of odd primes.

The main result of this paper is the following similar result of Theorem 1.3 for finite Euclidean graphs.

Theorem 1.4 *Consider the color set $L = \{c_1, \ldots, c_{q-1}\}$ coressponding to elements of $\mathbb{F}_q^*$. Color the complete graph K_{q^d} by the non-degenerate quadratic form Q as the above. Let $E \subset \mathbb{F}_q^d$, $d \geq 2$. Suppose that $1 \leq k - 1 \leq n \leq d$ and*

$$|E| \gg q^{\frac{d-1}{2}+k-1}. \tag{1.9}$$

Then for any subgraph H with k vertices and n edges with an arbitrary edge color distribution from L, we have

$$(1 + o(1))|E|^k q^{-n} \tag{1.10}$$

copies of H (with vertex ordering) in E.

The result is only non-trivial in the range $d \geq 2(k - 1)$. Note that Theorem 1.4 is stronger than Theorem 1.3 in this range. Moreover, different from Hart et al. [3], our proof uses probabilistic methods. The rest of this paper is organized as follows. In Section 2, we establish a theorem about the number of small colored subgraphs in pseudo-random coloring of a complete graph. Using this theorem, we give a proof of Theorem 1.4 and also discuss similar results in more general settings in the last section.

3

2 Pseudo-random coloring

We call a graph $G = (V, E)$ (n, d, λ)-graph if G is a d-regular graph on vertices with the absolute values of each of its eigenvalues but the largest one is at most λ. It is well-known that if $\lambda \ll d$ then a (n, d, λ) graph behaves similarly as a random graph $G_{n,d/n}$. Precisely, we have the following result (see Corollary 9.2.5 in [1]).

Theorem 2.1 *([1]) Let G be an (n, d, λ)-graph. For every set of vertices B and C of G, we have*

$$\left| e(B, C) - \frac{d}{n}|B||C\| \right| \leqslant \lambda \sqrt{|B||C|}, \tag{2.1}$$

where $e(B, C)$ is the number of edges in the induced bipartite subgraph of G on (B, C) (i.e. the number of ordered pairs (u, v) where $u \in B$, $v \in C$ and uv is an edge of G).

Let H be a fixed graph of order s with r edges and with automorphism group $\mathrm{Aut}(H)$. It is well-known that for every constant p the random graph $G(n, p)$ contains

$$(1 + o(1))p^r(1 - p)^{\binom{s}{2} - r} \frac{n^s}{|\mathrm{Aut}(H)|} \tag{2.2}$$

induced copies of H. Alon extended this result to (n, d, λ)-graph. He proved that every large subset of the set of vertices of a (n, d, λ)-graph contains the "correct" number of copies of any fixed small subgraph (Theorem 4.10 in [5]).

Theorem 2.2 *([5]) Let H be a fixed graph with r edges, s vertices and maximum degree Δ, and let $G = (V, E)$ be an (n, d, λ)-graph, where, say, $d \leqslant 0.9n$. Let $m < n$ satisfies $m \gg \lambda \left(\frac{n}{d}\right)^\Delta$. Then, for every subset $U \subset V$ of cardinality m, the number of (not necessarily induced) copies of H in U is*

$$(1 + o(1))\frac{m^s}{|\mathrm{Aut}(H)|} \left(\frac{d}{n}\right)^r. \tag{2.3}$$

Suppose that a graph G of order n is colored by t colors. Let G_i be the induced subgraph of G on the ith color. We call a t-colored graph G (n, d, λ)-r.c (regularly colored) graph if G_i is a (n, d, λ)-regular graph for each color $i \in \{1, \ldots, t\}$. We present here a variant of Theorem 2.2 that very large subset of the vertex set of a (n, d, λ)-r.c graph contains the "correct" number of copies of any fixed small colored graph.

Theorem 2.3 *Let H be a fixed t-colored graph with r edges, s vertices, maximum degree Δ with automorphism group (with respect to coloring) $\mathrm{Aut}_c(H)$, and let G be a t-colored graph of order n. Suppose that G is an (n, d, λ)-r.c graph, where, say, $d \ll n$. Let $m < n$ satisfies $m \gg \lambda \left(\frac{n}{d}\right)^\Delta$. Then, for every subset $U \subset V$ of cardinality m, the number of (not necessarily induced) copies of H in U is*

$$(1 + o(1))\frac{m^s}{|\mathrm{Aut}_c(H)|} \left(\frac{d}{n}\right)^r. \tag{2.4}$$

If we take the ordering of vertex set into account then the number of copies of H in U is

$$(1 + o(1))m^s \left(\frac{d}{n}\right)^r. \tag{2.5}$$

The proof of this theorem is similar to the proof of Theorem 4.10 in [5]. We give a detail proof here for the sake of completeness.

Proof To prove the theorem, consider a random one-to-one mapping of the set of vertices of H into the set of vertices U. Let $M(H)$ denote the event that every edge of H is mapped on an edge of K_n with corresponding color. We say that the mapping is an embedding of H in such a case. It suffices to prove that

$$\Pr(M(H)) = (1 + o(1)) \left(\frac{d}{n}\right)^r. \tag{2.6}$$

We prove (2.6) by induction on the number of edges r. The base case ($r = 0$) is trivial. Suppose that (2.6) holds for all colored graphs with less than r edges. Let uv be an edge of H. Let $H_u, H_v, H_{\{u,v\}}$ be the induced subgraph of H on the vertice set $V(H) - \{u\}$, $V(H) - \{v\}$, $V(H) - \{u, v\}$, and let H_{uv} be the graph obtained from H by removing the edge uv. We have

$$\Pr(M(H_{uv})) = \Pr(M(H_{uv})|M(H_{\{u,v\}})).\Pr(M(H_{\{u,v\}})). \tag{2.7}$$

Let r_1 be the number of edges of $H_{\{u,v\}}$. Since (2.6) holds for H_{uv} and $H_{\{u,v\}}$, we have $\Pr(M(H_{uv})) = (1 + o(1)) \left(\frac{d}{n}\right)^{r-1}$ and $\Pr(M(H_{\{u,v\}}) = (1 + o(1)) \left(\frac{d}{n}\right)^{r_1}$. Thus, we have

$$\Pr(M(H_{uv})|M(H_{\{u,v\}})) = (1 + o(1)) \left(\frac{d}{n}\right)^{r-r_1-1}. \tag{2.8}$$

For an embedding f_1 of $H_{\{u,v\}}$ in U, let $\phi(u, f_1)$, $\phi(v, f_1)$ and $\phi(uv, f_1)$ be the number of extensions of f_1 to an embedding of H_u, H_v and H_{uv} in U, respectively. Note that an extension f_u of f_1 to an embedding of H_u and an extension f_v of f_1 to an embedding of H_v give us a unique extension of f_1 to an embedding of H_{uv} except that the image of u in f_u is the same as the image of v in f_v. Thus, we have

$$\phi(u, f_1)\phi(v, f_1) - \min(\phi(u, f_1), \phi(v, f_1)) \leqslant \phi(uv, f_1) \leqslant \phi(u, f_1)\phi(v, f_1). \tag{2.9}$$

Averaging over all possible extensions of f_1 to a mapping from H_{uv} to U, we have

$$\frac{\phi(u, f_1)\phi(v, f_1) - \min(\phi(u, f_1), \phi(v, f_1))}{(m - s + 2)(m - s + 1)} \leqslant \Pr(M(H_{uv})|f_1) \leqslant \frac{\phi(u, f_1)\phi(v, f_1)}{(m - s + 2)(m - s + 1)}.$$

Taking expectation over all embedding f_1, the middle term becomes

$$\Pr(M(H_{uv})|M(H_{\{u,v\}})) = (1 + o(1)) \left(\frac{d}{n}\right)^{r-r_1-1}.$$

5

Note that $\min(\phi(u, f_1), \phi(v, f_1)) \leqslant m$ so we get

$$E_{f_1}(\phi(u, f_1)\phi(v, f_1)|M(H_{\{u,v\}})) = (1 + o(1))m^2 \left(\frac{d}{n}\right)^{r-r_1-1} + \delta,$$

where $|\delta| \leqslant m$. We have $r - r_1 \leqslant 2(\Delta - 1) + 1$ and $m \gg \lambda \left(\frac{n}{d}\right)^{\Delta} = \Omega(\sqrt{d})\left(\frac{n}{d}\right)^{\Delta}$, thus

$$m^2 \left(\frac{d}{n}\right)^{r-r_1-1} \geqslant m^2 \left(\frac{d}{n}\right)^{2(\Delta-1)} \gg \Omega(d)\left(\frac{n}{d}\right)^2 = \Omega(n^2/d) \gg n > m. \qquad (2.10)$$

So δ is negligible and we get

$$E_{f_1}(\phi(u, f_1)\phi(v, f_1)|M(H_{\{u,v\}})) = (1 + o(1))m^2 \left(\frac{d}{n}\right)^{r-r_1-1}. \qquad (2.11)$$

Now, let f be a random one-to-one mapping of $V(H)$ into U. Let f_1 be a fixed embedding of $H_{\{u,v\}}$. Let B and C be the set of all possible images of u and v over all possible extensions of f_1 to an embedding of H_u and H_v in U, respectively. Since G is an (n, d, λ)-r.c graph, by Theorem 2.1, the number of possible pairs (u, v) with $u \in B$ and $v \in C$ such that uv is correctly colored is bounded by

$$\frac{d}{n}\phi(u, f_1)\phi(v, f_1) \pm \lambda\sqrt{\phi(u, f_1)\phi(v, f_1)}. \qquad (2.12)$$

Thus, we have

$$\mathrm{Pr}_f(M(H)|f_{|V(H)\setminus\{u,v\}} = f_1) = \frac{d}{n}\frac{\phi(u, f_1)\phi(v, f_1)}{(m - s + 2)(m - s + 1)} + \delta,$$

where $|\delta| \leqslant \lambda\frac{\sqrt{\phi(u,f_1)\phi(v,f_1)}}{(m-s+2)(m-s+1)}$. Averaging over all possible embeddings f_1, we get

$$\begin{aligned}
\mathrm{Pr}(M(H)|M(H')) &= \frac{d}{n}\frac{E_{f_1}(\phi(u, f_1)\phi(v, f_1)|M(H_{\{u,v\}}))}{(m - s + 2)(m - s + 1)} + E_{f_1}(\delta) \\
&= (1 + o(1))\left(\frac{d}{n}\right)^{r-r_1} + E_{f_1}(\delta),
\end{aligned}$$

where the second lines follows from (2.12). By Jensen's inequality, we have

$$|E_{f_1}(\delta)| \leqslant \lambda\frac{\sqrt{E(\phi(u, f_1)\phi(v, f_1))}}{(m - s + 2)(m - s + 1)} = (1 + o(1))\frac{\lambda}{m}\left(\frac{d}{n}\right)^{(r-r_1-1)/2}, \qquad (2.13)$$

which is negligible to the first term (as $m \gg \lambda \left(\frac{n}{d}\right)^{\Delta} \geqslant \lambda \left(\frac{n}{d}\right)^{(r-r_1+1)/2}$). Thus, we have

$$\mathrm{Pr}(M(H)) = \mathrm{Pr}(M(H)|M(H_{\{u,v\}}))\,\mathrm{Pr}(M(H_{\{u,v\}})) = (1 + o(1))\left(\frac{d}{n}\right)^r. \qquad (2.14)$$

This completes the proof of the theorem. $\qquad\qquad\square$

6

3 Finite Euclidean graphs

3.1 Proof of Theorem 1.4

In [2], Bannai, Shimabukuro and Tanaka studied the spectrum of distance graph $G_q(a)$ and showed that these graphs are asymptotically Ramanujan graphs. They proved the following result.

Theorem 3.1 ([2, 7]) *Let Q be a non-degenerate quadratic form on $\mathbb{F}_q^d$. The finite Euclidean graph $E_q(d, Q, a)$ is regular of valency $(1 + o(1))q^{d-1}$ for any $a \in \mathbb{F}_q^*$. Let λ be any eigenvalues of the graph $G_q(a)$ with $\lambda \neq$ valency of the graph then*

$$|\lambda| \leq 2q^{\frac{d-1}{2}}. \tag{3.1}$$

From Theorem 3.1, if we color the complete graph $G = K_{q^d}$ with vertex set $\mathbb{F}_q^d$ by a non-degenerate quadratic form Q as in Section 1 then the colored graph G is a $(q^d, (1 + o(1))q^{d-1}, 2q^{\frac{d-1}{2}})$-r.c. graph. The Theorem 1.4 now follows immediately from Theorem 2.3.

3.2 General distances

The proof in [3] shows that the conclusion of Theorem 1.3 holds with the Euclidean norm $||.||$ is replaced by any function F with the property that the Fourier transform satisfies the decay estimates

$$\left| \hat{F}_t(m) \right| = \left| q^{-d} \sum_{x \in \mathbb{F}_q^d : F(x) = t} \chi(-x.m) \right| \leqslant Cq^{-(d+1)/2} \tag{3.2}$$

and

$$\left| \hat{F}_t(0, \ldots, 0) \right| = \left| q^{-d} \sum_{x \in \mathbb{F}_q^d : F(x) = t} \chi(-x.(0, \ldots, 0)) \right| \leqslant Cq^{-1}, \tag{3.3}$$

where $\chi(s) = e^{2\pi i \text{Tr}(s)/q}$ and $m \neq (0, \ldots, 0) \in \mathbb{F}_q^d$ (recall that for $y \in \mathbb{F}_q$, where $q = p^r$ with p prime, the trace of y is defined as $\text{Tr}(y) = y + y^p + \ldots + y^{p^{r-1}} \in \mathbb{F}_q$).

Now we define the F-distance graph $G_F(q, d, j)$ with the vertex set $V = \mathbb{F}_q^d$ and the edge set

$$E = \{(x, y) \in V \times V | x \neq y, F(x - y) = j\}.$$

Then the exponentials (or characters of the additive group $\mathbb{F}_q^d$)

$$e_m(x) = \exp\left(\frac{2\pi i \text{Tr}(x.m)}{p} \right), \tag{3.4}$$

for $x, m \in \mathbb{F}_q^d$, are eigenfunctions of the adjacency operator for the F-distance graph $G_F(q, d, j)$ corresponding to the eigenvalue

$$\lambda_m = \sum_{F(x)=j} e_m(x) = q^d \hat{F}_j(-m). \tag{3.5}$$

Thus, the decay estimates (3.2) and (3.3) are equivalent to

$$\lambda_m \leqslant C q^{(d-1)/2}, \tag{3.6}$$

for $m \neq (0, \ldots, 0) \in \mathbb{F}_q^d$, and

$$\lambda_{(0,\ldots,0)} \leqslant C q^{d-1}. \tag{3.7}$$

Therefore, we can apply Theorem 3.1 to obtain similar results.

Acknowledgements

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, 2nd ed., Willey-Interscience, 2000.

[2] E. Bannai, O. Shimabukuro and H. Tanaka, Finite Euclidean graphs and Ramanujan graphs, *Discrete Mathematics* (to appear).

[3] D. Hart, A. Iosevich, D. Koh, S. Senger and I. Uriarte-Tuero, Distance graphs in vector spaces over finite fields, coloring and pseudo-randomness, preprint (2008).

[4] A. Iosevich and M. Rudnev, Erdös distance problem in vector spaces over finite fields, *Trans. Amer. Math. Soc.*, (2007).

[5] M. Krivelevich and B. Sudakov, Pseudo-random graphs, *Conference on Finite and Infinite Sets Budapest*, Bolyai Society Mathematical Studies X, pp. 1–64.

[6] S. Li and L. A. Vinh, On the spectrum of unitary finite-Euclidean graphs, submitted to Ars Combinatoria (2008).

[7] A. Medrano, P. Myers, H. M. Stark and A. Terras, Finite analogues of Euclidean space, *Journal of Computational and Applied Mathematics*, **68** (1996), 221–238.

[8] L. A. Vinh and D. P. Dung, Explicit tough Ramsey graphs, *Proceedings of the International Conference on Relations, Orders and Graphs: Interaction with Computer Science*, Nouha Editions, 2008, 139-146.

[9] L. A. Vinh, Explicit Ramsey graphs and Erdös distance problem over finite Euclidean and non-Euclidean spaces, *The Electronic Journal of Combinatorics*, **15** (1), 2008, R5.

[10] L. A. Vinh, Szemeredi-Trotter type theorem and sum-product estimate in finite fields, submitted (2007).

[11] V. Vu, Sum-product estimates via directed expanders, *Mathematical Research Letters*, to appear.